MICHAEL BAILEY
United States Attorney
District of Arizona

KEVIN M. RAPP (Ariz. Bar No. 014249, kevin.rapp@usdoj.gov)
MARGARET PERLMETER (Ariz. Bar No. 024805, margaret.perlmeter@usdoj.gov)
PETER S. KOZINETS (Ariz. Bar No. 019856, peter.kozinets@usdoj.gov)
ANDREW C. STONE (Ariz. Bar No. 026543, andrew.stone@usdoj.gov)
Assistant U.S. Attorneys
40 N. Central Avenue, Suite 1800
Phoenix, Arizona 85004-4408
Telephone (602) 514-7500

JOHN J. KUCERA (Cal. Bar No. 274184, john.kucera@usdoj.gov)
Special Assistant U.S. Attorney
312 N. Spring Street, Suite 1200
Los Angeles, CA 90012
Telephone (213) 894-3391

BRIAN BENCZKOWSKI
Assistant Attorney General
Criminal Division, U.S. Department of Justice

REGINALD E. JONES (Miss. Bar No. 102806, reginald.jones4@usdoj.gov)
Senior Trial Attorney, U.S. Department of Justice
Child Exploitation and Obscenity Section
950 Pennsylvania Ave N.W., Room 2116
Washington, D.C. 20530
Telephone (202) 616-2807
Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

United States of America, Plaintiff, v. Michael Lacey, et al., Defendants.	No. CR-18-422-PHX-SMB **UNITED STATES' PRE-HEARING MEMORANDUM REGARDING DEFENDANTS' MOTION TO COMPEL (Doc. 643)** **Evidentiary Hearing: Oct. 3, 2019, 9:00 a.m., Courtroom: 506**

Introduction

The United States respectfully submits this Pre-Hearing Memorandum to identify the government's witnesses and their anticipated testimony at the October 3, 2019 hearing. As the testimony will show, the United States has produced to Defendants forensic copies of the computer servers that contained all then-existing data for all of the ads that were posted on www.backpage.com (the Backpage website) at the time the website was shut down on April 6, 2018. The United States produced this data in the same manner in which the United States possessed it, and in a format that is reasonably usable and searchable via industry-standard (and freely-available) database browser software, including MySQL. Using such software, the data can be searched and put into customizable reports displaying, *inter alia*: ad title, text and associated image location and file names; posting category and section; price and payment data; moderation logs; and whether the ad was flagged for inappropriate content. Defendants nevertheless claim that the fully-operational, live Backpage website provided more convenient access to this data, and they have essentially demanded that the government recreate the defunct website. If even possible, doing so would involve overcoming complex technological hurdles and significant time and expense, and would not provide any more information than that contained on the servers that the United States has already produced to the defense.[1]

In addition to the Backpage website servers and other server data, the United States has produced to date nearly eight million documents, including hundreds of thousands of internal Backpage business records (emails, PowerPoints, meeting agendas, financial analyses and other documents), in industry-standard, Relativity-compatible formats that

[1] For example, the operational Backpage website was a dynamic system that generated webpages in real-time from elements saved on different servers; as a result, the webpages as seen by Backpage's users were not saved as the users would have seen them. While it may not be possible to recreate the ads in the exact format in which they were displayed to users, the United States has preserved the underlying data used to create those ads (including ad title, text and associated images) and produced that data to the defense. Moreover, the United States has obtained historical copies (from local law enforcement and other sources) of the Backpage ads that are specifically identified in the Superseding Indictment, and has produced those ads to the defense.

are reasonably usable and searchable; produced subsets of "hot documents" relating to the allegations in the Superseding Indictment; met with counsel for several individual defendants to review the government's evidence; made available a Department of Justice discovery specialist to assist with technical questions; and provided extensive preliminary witness and exhibit lists more than a year before trial. (*See* Doc. 696, Resp. to Mot. to Compel at 1-2, 4-5, 11-15.) The vast majority of the United States' exhibits consist of documents that Backpage.com, LLC produced to the U.S. Senate Permanent Subcommittee on Investigations in 2016, and that were subsequently compelled to be produced as part of the grand jury investigation that led to the prosecution of this case. (*See* Doc. 696, Resp. to Mot. Compel at 4-5 and n.1; Doc. 444-1.) These documents evidence many of the business practices highlighted in the Superseding Indictment, including Backpage's: use of "moderation" to sanitize prostitution ads; aggregation of prostitution ads from competing websites; cross-linkage partnership with The Erotic Review, a prostitution review website; business arrangements with bulk prostitution advertisers like Dollar Bill; and money laundering practices. Several of these documents are discussed in the Senate Subcommittee's 50-page report BACKPAGE.COM'S KNOWING FACILITATION OF ONLINE SEX TRAFFICKING[2] and its 840-page appendix.[3]

The parties' briefing and oral argument on Defendants' Motion to Compel has raised a few key issues, including: (1) did the United States shut down the servers that ran the Backpage website in an appropriate manner such that the integrity of the data was maintained; (2) has the United States produced the website data it possesses; (3) was that data produced in a format that is reasonably usable and searchable; (4) can the United States reconstitute the Backpage website as it existed at the time of the shutdown; and (5) would

[2] Available at https://www.hsgac.senate.gov/imo/media/doc/Backpage%20Report%202017.01.10%20FINAL.pdf.

[3] Available at https://www.hsgac.senate.gov/imo/media/doc/Final%20Appendix%202017.01.09.pdf.

doing so provide the defense with any information that has not yet been produced? While recognizing the burden of proving materiality falls on Defendants pursuant to Fed. R. Crim. P. 16(a)(1)(E)(i), and without waiving the same, the United States proposes that these issues can be most efficiently addressed by permitting the government to open the October 3 hearing by calling the following witnesses identified below, and providing each side 15 minutes for summations at the close of all testimony.

Even though Defendants filed the motion and have the burden of proving their argument, they've raised issues with how the government collected and disclosed the website data. The government should be permitted to call its witnesses first to establish what it did when it shut down the website and produced the data. After the government has called its witnesses, then it would make sense for Defendants to put on their case to attempt to rebut the government's evidence. Defendants' expert, for example, will only testify as to what the government failed to do and how the government's collection and subsequent production of data was deficient. This argument makes more sense once the government has presented evidence on what it actually did. The government examining its witnesses first will be efficient and save time.

United States' Witnesses and Anticipated Testimony

1. FBI Special Agent and Forensic Examiner J. Patrick Cullen

Special Agent Cullen is a Forensic Examiner with the FBI's Phoenix Field Office. He was the agent in charge of the April 6, 2018 seizure of the Backpage website servers operated by DesertNet and located at the Login, Inc. Data Center in Tucson. It is anticipated that Special Agent Cullen will testify as follows:

On April 6, 2018, at his direction and the supervision, DesertNet personnel powered down the Backpage website servers at the Login, Inc. Data Center in an orderly fashion, and then unracked the servers so that they could be removed and transported an FBI facility for forensic examination and, if appropriate, imaging. DesertNet utilized a "soft" shut down to power-down the website.

In cases involving the seizure of electronically stored information (ESI), there is always a continuum between preservation and convenience. In this case, and consistent with FBI e-discovery practices, the FBI erred on the side of preservation by directing DesertNet to power-down the Backpage website servers. This preserved the servers against further changes that would have been made by keeping them powered-on. Even if the servers had been disconnected from the internet, if powered-on they would have continued to run regularly-scheduled programming routines that deleted old data (such as data relating to expired ads) and made other changes. Powering-down the servers ensured that the server data as it existed on April 6, 2018 would be frozen in time and preserved for future analysis. Moreover, because it was not practicable to conduct forensic examination (and, if warranted, imaging) of the Backpage servers on-site, DesertNet personnel unracked the servers so that they could prepared for transportation to an appropriate FBI facility.

2. Wil Gerken

Mr. Gerken is the Chief Technology Officer of DesertNet, a Tucson-based technology vendor that has administered the computer servers that ran the Backpage website since Backpage's inception in 2004.[4] Mr. Gerken was Backpage's primary contact at DesertNet regarding the operation of the website. It is anticipated that he will testify as follows:

a. Configuration of the Backpage Website Servers

DesertNet maintained the Backpage website servers at two datacenters—the Login, Inc. Data Center in Tucson, and the Switch Data Center in Amsterdam. For website reliability and disaster recovery purposes, the servers at the two datacenters were entirely redundant, and the website could be run out of either datacenter.[5]

[4] As averred by Backpage.com's Chief Information Officer, Chris Kempel, Backpage outsourced the development and management of its advertising data servers to DesertNet. DesertNet handled the management of all Backpage data that had to do with displaying advertisements, including advertisements, photos, text, banner ads, etc. None of this data resided at Backpage. (*See* Doc. 739-1, Decl. of Chris Kempel in Supp. of Mot. to Quash Subpoena on Carl Ferrer ¶ 4.)

[5] A "server" is "a computer that provides data to other computers….[¶] Many types of servers exist, including web servers, mail servers, and file servers. Each type runs software specific to the purpose of the server….[¶] [M]ost large businesses use rack-mountable hardware designed specifically for server functionality…. Multiple rack-mountable

To further protect the website, each datacenter had massive internal redundancies. For example, each datacenter had one "master" database server and at least three "slave" or database servers that contained the same data as the master database server. Whenever any new ad data was added to the Backpage website, the data was "written" or saved to a master database server and then replicated to the slave database servers. The master database was the primary or definitive source of data if there was any lag between the database servers. The copying of data from the active master to the redundant databases (called "replicating") occurred in a matter of milliseconds. To optimize the performance of the website, the slave servers (which could "scale" or handle increased website traffic more easily than the master servers) typically supplied the data that would be fetched (or "read") by the website.

Because images files (photos, videos, etc.) use more storage than other types of data, it typically is not efficient to store images on a database server. Accordingly, the images that appeared in Backpage's ads were stored on separate image servers. The database servers contained "pointers" to the image files that were to be used with each particular ad. There were three image servers in Amsterdam and three image servers in Tucson. An image uploaded by a Backpage user would be sent to one of the three servers randomly and then file-synced to the other two image servers. Because of this, any one of the image servers contained all of the image files associated with all of the then-existing ads posted on the Backpage website.

The Amsterdam and Tucson datacenters also had one or more backup servers that did not contain any data that was not also contained on the master database server and image servers described above. In addition, the Amsterdam facility housed "Payment Processing Island" (PPI) servers that contained certain types of transaction-based data, such as information relating to credit cards, cryptocurrencies, credits or other forms of payment used for particular ad purchases. In part to comply with Payment Card Industry

servers can be placed in a single rack and often share the same monitor and input devices." https://techterms.com/definition/server (last visited Sept. 26, 2019).

Security Standards and other data privacy laws, Backpage limited the amount and types of payment and personal data that it stored on the PPI servers, and Backpage had a policy of purging transactional data after a given time. DesertNet was not involved in running or maintaining the PPI servers; those servers were managed directly by Backpage.com, LLC. In all events, certain payment information associated with particular ads was also stored on the database servers discussed above—this information includes ad price, transaction approval data, reference numbers, and date and time stamps.

Simply put, because of the massive redundancy built into the configuration of the Backpage website, all of the data for the ads posted on the website at any given time could be found in any one database server and any one image server. If the website was brought up and running again, it may provide a more convenient way to view the data, but it would not have any more information than would be contained in one database server and one image server.

b. Further Details Regarding Data Stored on the Database Servers

The master database server contained both a "central database" and "market databases." The central database contained information pertinent to the entirety of Backpage's website, including filters that were applied to all ads, and a site table that listed each market in which Backpage operated. (*See* Doc. 626-4 at 13.) The central database also contained some data relating to ads that were moderated or edited by Backpage, including the ad text. However, the central database did not include all of the data associated with moderated ads, or older versions of the moderated ad's text. Stated differently, there was no "versioning" built into the system: once ad text was changed, the new text replaced or overwrote the old text—the old text was not saved. If images were deleted from an ad, the old images would remain on the image server and remain associated with the ad, but the images would be flagged for exclusion from the ad when the webpage for the ad was generated by a web server.[6]

The central database also contained a "site" table that listed the name of every individual market database and the groupings of the market databases. Market databases were created for each state, city or region in which Backpage operated, and were designated with names such as "nyc_backpage" or "phx_backage." The market databases contained all data that an advertiser provided for each particular ad, except for the image files (which were stored on the image servers). When a user originally posted an ad, the data for the ad (including the ad text) would be written to the pertinent market database on the master server.

c. Accessing or Reassembling the Website Data

The live, operational Backpage website was produced by three active servers working together: (i) a database server; (ii) an image server; and (iii) a web server. A web server would fetch data from the database and image servers to dynamically generate webpages for display on the internet. The web servers themselves did not store any content or images, or retain any unique data; they merely put data from the database and image servers into displayable webpages. For example, rather than store any image files, the web servers would point to the images stored on the image servers, and the image servers would serve the images to the webpage being displayed to the user in real time. As a result, any given ad was not saved on any of the servers as a user would have seen it.

Reassembling a fully-functioning version of the website that operates just like the live version would be a difficult, technologically-challenging task. Because links and references to files and data within the servers were referenced based on the way that the servers were networked when the website was operational, restoring the website to a

[6] At the time that the government applied for a search warrant for the Tucson datacenter servers, the government had a good faith belief that the serves may have contained historical versions of ads that were later edited through the moderation process. (*Cf*. Doc. 643, Mot. to Compel at 3-4.) Upon obtaining and examining the servers, the government learned that this was not the case. (*See* Doc. 696, Resp. to Mot. to Compel at 13.)

functional state is not as simple as connecting any three servers of the appropriate types. Rather, the IP (Internet Protocol) addresses of the different servers as they were configured at that time would need to be rediscovered, and the organization and interrelationship of the various system components would need to be reconstructed. There would be a need to programmatically merge various system components and have them work together in concert to pull data from the right places at the right times to make the website look exactly as it would have appeared (to outside users and internal administrators) when the website was operational. This is a technologically complex task that would likely involve considerable time and cost to accomplish.

Rather than recreate a website that no longer exists, it would be much easier and quicker to pull the existing website data into a new interface. A specialist provided with forensic copies of one master database server and one image server would be able to identify the data and images associated with each ad that existed on the Backpage website at the time of the shutdown, provided that the specialist was proficient in MySQL—the version of Structured Query Language used in the master database; FreeBSD (Berkeley Software Distribution)—the operating system that the servers used; ZFS (Z File System)—the file system used to store the data on the servers; and APACHE Web Server—free, open-source web server software.

d. The Shutdown of the Backpage Website Servers

On April 6, 2018, at the direction and under the supervision of the FBI, DesertNet personnel powered down the Backpage servers at the Login, Inc. Data Center in an orderly fashion, and then unracked the servers so that they could be removed and transported by the FBI to another location for forensic examination. DesertNet personnel were in the best position to power-down and un-rack the servers because they were responsible for running and maintaining the servers, and DesertNet was the only company with access and knowledge to perform these functions appropriately.

3. FBI Information Technology Specialist-Forensic Examiner Matt Frost

Mr. Frost has been part of the FBI's Computer Analysis and Response Team (CART) for 10 years. His specialization and experience includes MySQL database systems and Z File System storage. It is anticipated that Mr. Frost will testify as follows:

a. The Government's Production of Backpage's Website Servers

Mr. Frost became involved with the Backpage case after the Backpage website was shut down. The FBI assigned him to assist with the processing, analysis and imaging of the servers it had recently seized. In late April or early May 2018, Mr. Frost reviewed in Phoenix the servers that the FBI had seized from DesertNet. Mr. Frost previewed the servers and identified the master database server and an image server. These two servers were then sent to the FBI facility in Pocatello, Idaho (where Mr. Frost is based). Mr. Frost created mirror-image copies (forensic copies) of these two servers and put them onto hard drives for production to the defense. Mr. Frost subsequently received four servers from Amsterdam (the master database server, a duplicate of the master database server, a slave database server, and an image server), created forensic copies of these servers, and put them onto hard drives for production to the defense. While each server could contain up to 24 physical hard drives, Mr. Frost consolidated the servers into a smaller number of hard drives (56) saved in industry-standard E01 format (also called "Expert Witness Format").[7] Due to the volumes of the data involved, this process took several months to accomplish.

In February 2019, Mr. Frost participated in a teleconference with government prosecutors, other FBI representatives, and certain defense representatives. Mr. Frost explained how the government would be producing the website server data. The defense representatives did not object to the proposed production format, nor did they request

[7] E01 is an industry-standard format used in the production of forensic copies of electronically stored information. As one website explains: "Encase Forensic is the most widely known and used forensic tool…. [W]hen Encase is used for creating backup (i.e. Imaging) of hard drives…a file known as 'E01' is produced. This '.e01' extension file is primarily recognized as 'Encase Image File Format'. The E01 image file format is also known as EWF (an acronym for Expert Witness Format)." http://www.forensicsware.com/blog/e01-file-format.html (last visited Oct. 1, 2019).

production in an alternative format.

On March 8, 2019, these hard drives were produced to the defense. This production included all data and images relating to all of the ads that were on the Backpage website at the time of the April 6, 2018 shutdown.[8]

In addition, on March 11, 2019, the government produced a separate hard drive that contained the extracted database files from the master database server, saved in .sql format. By doing so, the government had taken the extra step of making the master database server data easier to use, because .sql files can be easily imported into freely-available database browser software and readily searched. Mr. Frost had informed the defense that the government would be taking this extra step during the February 2019 teleconference.

Moreover, on March 14, 2019, the government produced a DVD that contained extracted data and pictures associated with the ads identified in the Superseding Indictment.

b. The Government Produced the Website Server Data in a Reasonably Usable and Searchable Format

Defendants claim that the Backpage server data has been produced to them in an unusable and nonfunctional format. However, using HeidiSQL (a MySQL database browser that can be downloaded for free[9]), the data can be easily searched and used to provide customizable database reports. Illustratively, using HeidiSQL, Mr. Frost prepared the spreadsheet attached as Exhibit J to Defendants' Motion to Compel (Doc. 643-11, Exhibit J). The spreadsheet is a printout of the ad data saved on the master database server for one of the ads referenced in the Superseding Indictment. These fields included the following:

Objid	creationdate	lastmodified	lastedituser

[8] Also on March 8, 2019, the government produced forensic copies of two servers from Backpage's offices in Dallas. Mr. Frost was not involved in imaging and producing the Dallas servers.

[9] https://www.heidisql.com/ (last visited Oct. 1, 2019).

id	partner	category	section
Postingdate	postingtime	expirationdate	sponsorreleasedate
sponsorexpirationdate	sponsorplacement	sponsored	sponsortagline
Status	user	email	smsenabled
Contactphone	allowreplies	showadlinks	joineddate
header [title of the ad]	ad [text of the ad]	hasimage	hasvideo
autoreplyimage	autoreplymessage	regionother	roommates
Units	age	price	education
Salary	maddress	mazip	feespaidby
Adplacedby	url	ip	proxyscore
Isp	org	browserlanguage	countrycode
Country	city	searchblob	tier
Onlineprice	printprice	sponsorprice	adprice
Paytype	approval code[10]	idstamp	cardref
Promotioncode	invoicedescription	lastviolation date	violationcount
violation[11]	timetorepost	repostcycle	nextrepost
Repostime	timestomovetotop	nextmovetotop	sortkey
Globalreport	localscore	localreport	moderation[12]
moderationlog[13]	centralserverupdate	permalink	displaydisclaimer
sponsoradlayout[14]	movetotopreminder	basename	publishtime

[10] This field encompasses transaction information, such as "APPROVED," reference numbers, and dates and times.

[11] This field includes additional data or text such as "hits," "action," "flag as spam," and "match."

[12] This field indicates if an ad was "Reviewed."

[13] This field indicates if an ad was "Approved," provides identification codes for the moderator who approved the ad, provides a date and time stamp.

[14] This field includes layout instructions and image pointers.

(*See* Doc. 643-11, Mot. to Compel, Exhibit J.) As discussed above, Mr. Frost provided spreadsheets containing these fields for ads identified in the Superseding Indictment.

Mr. Frost will also explain how additional Backpage ad data searches can be performed, and how associated ad images can be located.

c. Recreating the Backpage Website Is Neither Practicable Nor Necessary

Even though any database-image server pair from the Tucson or Amsterdam datacenter would have contained all then-existing data for all of the ads on Backpage's system at the time the website was taken down on April 6, 2018, recreating or simulating all functionality available on the website as it then-existed would require extensive time, expenditure and expertise (if possible at all).

The government had endeavored to pursue a two-track approach to preserving the Backpage website. First, the FBI followed its established ESI collection practices in achieving an orderly powering-down of the website servers in the Tucson datacenter, and in transferring the servers to an appropriate FBI facility for forensic examination and, where warranted, imaging. This would ensure the preservation of the data saved on the Backpage website servers, without risking any alteration of the data that would have occurred by powering the servers back on.

Second, the FBI had hoped to keep the Amsterdam data center servers in place and capable of being operated remotely to assist with other law enforcement investigations, including investigations relating to human- and sex-trafficking victims who had been sold on Backpage. Unfortunately, in June 2018, after learning that Backpage and its CEO had pleaded guilty, Dutch authorities refused to allow the Amsterdam servers to remain in place and operable within Dutch territory.

Legal Analysis

I. The Government Has Produced the Unique Website Data that It Possesses in a Reasonably Usable Industry-Standard Format.

Fed. R. Crim. P. 16(a)(1)(E) provides that on a defendant's request, the government must permit the defendant to inspect . . . data, . . .tangible objects, . . . or copies or portions of any of these items, if the item is within the government's possession, custody, or control" and "the item is material to preparing the defense." Moreover, in 2012, the Administrative Office of the U.S. Courts published "Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases," available at http://www.uscourts.gov/sites/default/files/finalesiprotocolbookmarked.pdf (the "ESI Protocol"). The ESI protocol states that (1) the parties should meet at the outset of the case and periodically continue to discuss "what formats of production are possible and appropriate….Any format selected for producing discovery should maintain the ESI's integrity, allow for reasonable usability, and reasonably limit costs, and, if possible, conform to industry standards for the format"; and (2) that "[w]hen producing ESI discovery, a party should not be required to take on substantial additional processing or formatting conversion costs and burdens beyond what the party has already done or would do for its own case preparation or discovery production." ESI Protocol, Introduction at 1-2 (summarizing Principles 4 and 5).

Courts widely recognize that the government has no duty to produce discovery in a format it does not have. *United States v. Gray*, 648 F.3d 562, 567 (7th Cir. 2011) ("Having turned over the underlying data, the prosecutors had no duty to go further and conduct the defense's investigation for it"; holding that government had no duty to create and run programs to extract data from its database that would be useful to the defense); *United States v. Budovsky*, 2016 WL 386133, at *12 (S.D.N.Y. 2016) ("There is no basis to find here that the government was obliged to produce the discovery to defense in a format that the government did not have."); *see also* ESI Protocol Principle 5 ("When producing ESI, a party should not be required to take on substantial additional processing or formatting costs and burdens beyond what the party has already done or would do for its own case preparation or discovery production.").

Further, the ESI Protocol makes clear that ESI should be produced either in the format in which it was received—or in a reasonably usable format: "ESI received from third parties should be produced in the format(s) it was received or in a reasonably usable format(s). ESI from the government's or defendant's business records should be produced in the format(s) in which it was maintained or in a reasonably usable format(s)." ESI Protocol Principle 6(b). The ESI Protocol also suggests that, even if a case involves millions of pages of discovery, the government does not have any special *Brady* obligations so long as it produces the ESI in a searchable format, provides a table of contents, and produces a subset of "hot" documents." ESI Protocol, Strategies at 2 & n.1.

As the testimony will show, the government met and conferred with defense counsel in February 2019 before producing forensic copies of the Backpage website servers. The government's forensic expert, Matt Frost, participated in the call and explained how the server data would be produced. Mr. Frost also recommended that the defense make use of the .sql database files that would be produced on a separate, stand-alone hard drive (and that can be easily imported into a MySQL database browser). The defense did not object and did not request production in any alternative formats.

In March 2019, the government produced to the defense the same unique Backpage website server data that the government possessed—namely, industry-standard forensic copies of a master database server and an image server. To make the data more accessible and easier to use, the government also created and produced to the defense a separate hard drive containing database files in .sql format. The .sql files can be loaded into a free database browser and easily searched and queried. Moreover, the government provided a separate DVD that contained the ad data and images for the ads identified in the Superseding Indictment. Consistent with Rule 16 and the ESI Protocols, the government met and exceeded its discovery obligations regarding the Backpage website servers.

II. The Relief Sought by Defendants Should Be Denied.

The government should not be required to recreate a website that no longer exists, especially where—as here—Defendants have been provided with all of the unique underlying website data that the government possesses, in an industry-standard format that is reasonably usable and searchable. Recreating a fully-operational version of the Backpage website as it existed on the day of the website's shut down would involve overcoming a number of complex technical issues, and considerable expense and time. It would not provide the defense with any more data than what the government has already produced. But it would significantly delay trial.

Nor should the government be ordered to produce the 28 categories of information that Defendants have requested. (*See* Doc. 643, Mot. to Compel at 7-8, 16-17 and Exhibit B.) As Judge Logan previously found, the law does not require the government to conduct Defendants' work for them. (*See* Doc. 339 at 5 ("The government is under no general obligation to identify *Brady* or *Giglio* material within voluminous discovery.").) For these reasons, and for the reasons more fully set forth in United States' Response to the Motion to Compel (incorporated fully herein by this reference), Defendants' Motion should be denied. (*See* Doc. 696, Resp. to Mot. to Compel at 10-11); *see also Rhoades v. Henry*, 638 F.3d 1027, 1039 and n.12 (9th Cir. 2011) (the government is not "obliged to sift fastidiously" through millions of pages (whether paper or electronic)); *United States v. Warshak*, 631 F.3d 266, 297 (6th Cir. 2010); *United States v. Skilling*, 554 F.3d 529, 576 (5th Cir. 2009) (The government is "under no duty to direct a defendant to exculpatory evidence [of which it is unaware] within a larger mass of disclosed evidence.").

Conclusion

Defendants' Motion (Doc. 643) should be denied.

Respectfully submitted this 2nd day of October, 2019.

MICHAEL BAILEY
United States Attorney
District of Arizona

s/ Kevin M. Rapp

KEVIN M. RAPP
MARGARET PERLMETER
PETER S. KOZINETS
ANDREW C. STONE
Assistant U.S. Attorneys

JOHN J. KUCERA
Special Assistant U.S. Attorney

BRIAN BENCZKOWSKI
Assistant Attorney General
U.S. Department of Justice
Criminal Division, U.S. Department of Justice

REGINALD E. JONES
Senior Trial Attorney
U.S. Department of Justice, Criminal Division
Child Exploitation and Obscenity Section

CERTIFICATE OF SERVICE

I hereby certify that on October 2, 2019, I electronically transmitted the attached document to the Clerk's Office using the CM/ECF System for filing and transmittal of a Notice of Electronic Filing to the CM/ECF registrants who have entered their appearance as counsel of record.

s/ Angela Schuetta
Angela Schuetta
U.S. Attorney's Office